The New York Times
nytimes.com

November 9, 2003

Machine Politics in the Digital Age

By MELANIE WARNER

IN mid-August, Walden W. O'Dell, the chief executive of Diebold Inc., sat down at his computer to compose a letter inviting 100 wealthy and politically inclined friends to a Republican Party fund-raiser, to be held at his home in a suburb of Columbus, Ohio. "I am committed to helping Ohio deliver its electoral votes to the president next year," wrote Mr. O'Dell, whose company is based in Canton, Ohio.

That is hardly unusual for Mr. O'Dell. A longtime Republican, he is a member of President Bush's "Rangers and Pioneers," an elite group of loyalists who have raised at least $100,000 each for the 2004 race.

But it is not the only way that Mr. O'Dell is involved in the election process. Through Diebold Election Systems, a subsidiary in McKinney, Tex., his company is among the country's biggest suppliers of paperless, touch-screen voting machines.

Judging from Federal Election Commission data, at least eight million people will cast their ballots using Diebold machines next November. That is 8 percent of the number of people who voted in 2000, and includes all voters in the states of Georgia and Maryland and those in various counties of California, Virginia, Texas, Indiana, Arizona and Kansas.

Some people find Mr. O'Dell's pairing of interests - as voting-machine magnate and devoted Republican fund-raiser - troubling. To skeptics, including more than a few Democrats, it raises at least the appearance of an ethical problem. Some of the chatter on the Internet goes so far as to suggest that he could use his own machines to sway the election.

Senator Jon Corzine, Democrat of New Jersey, does not buy such conspiracy theories, but he said he was appalled at the situation.

"It's outrageous," he said. "Not only does Mr. O'Dell want the contract to provide every voting machine in the nation for the next election - he wants to 'deliver' the election to Mr. Bush. There are enough conflicts in this story to fill an ethics manual."

Mr. O'Dell declined to be interviewed for this article, but a company official said that his political affiliations had nothing to do with Diebold's operations, and that the company derived the bulk of its revenue from A.T.M.'s, not voting machines. "This is not Diebold; this is Wally O'Dell personally," said Thomas W. Swidarski, senior vice president for strategic development and global marketing at Diebold, who works closely with Mr. O'Dell. "The issue has been misconstrued."

BUT the controversy surrounding Diebold goes beyond its chief executive's political activities. In July, professors at Johns Hopkins University and Rice University analyzed the software code for the company's touch-screen voting machines and concluded that there was "no evidence of rigorous software engineering discipline" and that "cryptography, when used at all, is used incorrectly."

Making matters worse, the software code for the machines was discovered in January by a Seattle-area writer on a publicly accessible Internet site. That the code was unprotected constitutes a significant security lapse by Diebold, said Aviel D. Rubin, an associate professor of computer science at Johns Hopkins, co-author of the study of the code.

Mr. Swidarski said the code on the Internet site was outdated and was not now in use in machines.

About 15,000 internal Diebold e-mail messages also found their way to the Internet. Some referred to software patches installed on Diebold machines days before elections. Others indicated that the Microsoft Access database used in Diebold's tabulation servers was not protected by passwords. Diebold, which says passwords are now installed on machines, is threatening legal action against anyone who posts the files or links to them, contending that the e-mail is copyrighted.

A recent report for the state of Maryland by SAIC, an engineering and research firm, has added to concerns about the security of Diebold's systems. It recommended 17 steps that Maryland election officials could take to ensure better security when using Diebold's machines.

The company seized upon this as evidence that its systems, if used properly, were secure. But the report's overall assessment was not particularly upbeat. "The system, as implemented in policy, procedure and technology, is at high risk of compromise," SAIC wrote.

It has been a bumpy couple of months for Mr. O'Dell, 58, who is known as Wally and spent 33 years at Emerson Electric before joining what is now Diebold Election Systems. Associates say he was stunned by the reaction to his August letter and now regrets writing it.

"Wally's going to take a lower profile on this stuff," Mr. Swidarski said. But Mr. Swidarski did not indicate that Mr. O'Dell would put a halt to all of his political activities. Those have included attendance at a Bush fund-raiser in Cincinnati on Sept. 30 and a flight to Crawford, Tex., in August for a Pioneers and Rangers meeting attended by the president.

Other Diebold executives have contributed to President Bush's re-election campaign. According to data reported to the Federal Election Commission, 11 executives have added a total of $22,000 to the president's campaign coffers this year. No money from Diebold or its executives has gone to Democratic presidential candidates this year.

The controversy over security has started to affect Diebold's business. Last week, the office of the California secretary of state halted certification of Diebold's latest touch-screen voting machines, which individual counties are considering using. In Wisconsin, security concerns have soured election officials' perceptions of computerized voting. "We were already not strongly in favor of it, but the whole problem has changed when you're getting e-mails every week saying, 'You're not going to do this, right?' " said Kevin J. Kennedy, director of Wisconsin's election board.

Matt Summerville, an analyst at McDonald Investments in Cleveland, said the California decision could cause Diebold to book less revenue in its voting division this year than it had hoped. "It has certainly made their business a little more challenging," said Mr. Summerville, who expects the voting division to contribute $113 million this year to Diebold's total revenue of $2.1 billion.

So far, investors have not seemed concerned. Diebold's stock is up almost 36 percent for the year.

Until recently, Diebold's voting business looked extremely promising. Florida's electoral fiasco in 2000 confirmed what many state and county election officials had known for years: that punch-card systems were outdated. Encouraged by a new federal law that set aside $3.9 billion for voting improvements, many states and counties are moving rapidly to computer-based systems.

Analysts say the biggest beneficiaries of the federal dollars are likely to be Diebold, Election Systems & Software in Omaha and Sequoia Voting Systems, based in Oakland, Calif. So far, Washington has provided $650 million to states to buy new voting machines and improve the election process, though most of that has yet to be spent. An additional $830 million is waiting to be disbursed as soon as a new national oversight committee for elections is established.

NOT everyone is convinced that spending hundreds of millions of dollars to computerize the nation's voting is a good thing. The Johns Hopkins and SAIC reports are part of a growing chorus of criticism about the reliability and safety of paperless voting systems.

"There's a feeling in the computer scientist community of utter dismay about the state of voting-machine technology," said Douglas W. Jones, an associate professor of computer science at the University of Iowa and a member of Iowa's board of examiners for voting machines.

David L. Dill, a computer science professor at Stanford, said: "If I was a programmer at one of these companies and I wanted to steal an election, it would be very easy. I could put something in the software that would be impossible for people to detect, and it would change the votes from one party to another. And you could do it so it's not going to show up statistically as an anomaly."

Diebold says there are enough checks and balances in the system to catch this. "Programmers do not set up the elections; election officials do," Mr. Swidarski said. "All a programmer knows are numbers, which are not assigned to real people and parties until set-up time."

But Professor Dill says the inherent complexity of software code makes it nearly impossible to ensure that computerized elections are fair. He advocates that machines be required to print out a paper ballot, which voters can use to verify their selections and which will serve as an audit trail in the event of irregularities or recounts.

Touch-screen machines from Diebold, called AccuVotes, do not have such a "voter verified" paper trail. ES&S and Sequoia are working on prototypes for machines with printers. Diebold's machines are like A.T.M.'s, in that voters touch their selection and hit "enter" to record their votes onto memory cards inside each terminal. After voting has ended, the memory cards are inserted into a Diebold server at each precinct. The results are tabulated and sent by modem, or the data disks are sent to a central office.

Rebecca Mercuri, a computer scientist and president of the consulting firm Notable Software, who has been studying election systems for 14 years, says the trouble with this system is that it is secretive. It prohibits anyone from knowing whether the data coming out of the terminals represents what voters actually selected. If someone were to challenge election results, the data in memory cards and the software running the voting terminals could be examined only by Diebold representatives.

MS. MERCURI ran up against this last year, when she served as a consultant in a contested city council election in Boca Raton, Fla. Her request to look at the software inside the city's machines, made by Sequoia, to see if there were any bugs or malfunctions, was denied by a judge on the grounds that the technology was protected by trade-secret clauses. Sequoia, ES&S and Diebold routinely include such clauses in their contracts.

"These companies are basically saying 'trust us,' " Ms. Mercuri said. "Why should anybody trust them? That's not the way democracy is supposed to work."

Representative Rush D. Holt, Democrat of New Jersey, is leading an effort to make computerized voting more transparent. His bill, introduced this year, would require that computerized voting systems produce a voter-verified paper ballot and that the software code be publicly available.

The bill, in the House Administration Committee, has 60 co-sponsors, all Democrats.

"Someone said to me the other day, 'We've had these electronic voting machines for several years now and we've never had a problem.' And I said, 'How do you know?' and he couldn't answer that," Representative Holt said. "The job of verification shouldn't belong to the company; it should belong to the voter."

Diebold said it would be willing to attach ballot printers to touch-screen machines if customers wanted them. But Mr. Swidarski said elections boards were not clamoring for it. "We're agnostic to it," he said.

Mr. Swidarski disputed the assertion that Diebold's systems are vulnerable to tampering. Before each election, he said, the software goes through rigorous testing and certification by one of three companies contracted through the National Association of State Election Directors. Those companies "go through every line of code," he said. "It's an extensive process that takes several months, and then the machines go for testing at the state level."

Critics say that the certification process is not as thorough as the companies would have people believe, and that the resulting reports, like the technology, are not available for public inspection. This opacity is what worries detractors most.

"We know from Enron and WorldCom that when accounting is weak, crooks have been known to take over," Professor Jones said. "If vulnerabilities exist in any voting system for a long enough time, someone's going to exploit it."